PENDING CLAIMS AS AMENDED

Please amend the claims as follows:

1. (Currently Amended) A method of validating an association of software code with [[for]] hardware, comprising:

obtaining a certificate from a code image, wherein:

the code image further including software code, a code signature, and a first identifier associated with a release of the software code,

all instances of the software code associated with the software release have the same first identifier such that at least two instances of the software code have the same first identifier,

the code signature is generated, using cryptography and a code private key, based on the first identifier, a second identifier for the hardware, and a message code digest obtained by hashing the software code,

the code signature is used to validate an association of the software code with the hardware,

the certificate includes a code public key corresponding to the code private key, and an authority signature generated over the code public key using cryptography and an authority private key;

authenticating the [[a]] certificate~~, included in a code image,~~ with an authority ~~first~~ public key securely stored in the hardware~~, the code image further including the software~~;

obtaining the first identifier from the code image;

obtaining the second identifier for the hardware, wherein all instances of a particular configuration of the hardware have the same second identifier such that at least two instances of the hardware have the same second identifier;

obtaining the software code from the code image and generating an image code digest by hashing the software code from the code image;

generating a regenerated signature digest by hashing the image code digest, the first identifier, and the second identifier; and

obtaining the code [[a]] signature[[,]] from the code image and generating a received signature digest by decrypting the code signature from the code image using the code public key ~~certificate, generated for the software, a first identifier for the software, and a second identifier for the hardware, wherein the signature is generated using cryptography and is used to validate an association of the software with the hardware~~; and

comparing ~~validating~~ the regenerated signature digest with the received signature digest ~~a second public key from the certificate~~, wherein the association of the software code with the hardware is validated if the regenerated signature digest matches the received signature digest ~~is validated~~.

2. (Currently Amended) The method of claim 1, wherein the software code is executed by the hardware only if the association is validated.

3. (Canceled)

4. (Canceled)

5. (Currently Amended) The method of claim 1, wherein the regenerated signature digest is generated using a cryptography scheme that includes Hash-based Message Authentication Code (HMAC).

6. (Original) The method of claim 1, wherein the first identifier is a software release version number.

7. (Original) The method of claim 1, wherein the hardware is an integrated circuit of a specific design.

8. (Currently Amended) The method of claim 1, wherein the second identifier is a hardware ~~serial number or~~ part number.

9. (Currently Amended) An apparatus having validation of an association of software with the apparatus [[for]] hardware, comprising:

a first storage unit configured to securely store an authority ~~a first~~ public key; and

a processor operative to

obtain a certificate from a code image, wherein:

the code image further including software code, a code signature, and a first identifier associated with a release of the software code,

all instances of the software code associated with the software release have the same first identifier such that at least two instances of the software code have the same first identifier,

the code signature is generated, using cryptography and a code private key, based on the first identifier, a second identifier for the hardware, and a message code digest obtained by hashing the software code,

the code signature is used to validate an association of the software code with the hardware,

the certificate includes a code public key corresponding to the code private key, and an authority signature generated over the code public key using cryptography and an authority private key;

authenticate the [[a]] certificate~~, included in a code image,~~ with the authority ~~first~~ public key ~~where the code image further include the software~~;

obtain the first identifier from the code image;

obtain the second identifier for the hardware, wherein all instances of a particular configuration of the hardware have the same second identifier such that at least two instances of the hardware have the same second identifier;

obtain the software code from the code image and generate an image code digest by hashing the software code from the code image;

generate a regenerated signature digest by hashing the image code digest, the first identifier, and the second identifier; and

obtain the code [[a]] signature [[,]] from the code image and generate a received signature digest by decrypting the code signature from the code image using the code public key ~~certificate, generated for the software, a first identifier for the software, and a second identifier for the hardware, wherein the signature is generated using cryptography and is used to validate an association of the software with the hardware~~; and

compare ~~validate~~ the regenerated signature digest with the received signature digest ~~a second public key from the certificate~~, wherein the association of the software code with the hardware is validated if the regenerated signature digest matches the received signature digest ~~is validated~~.

10. (Canceled)

11. (Currently Amended) The apparatus of claim 9, further comprising:

a second storage unit configured to store boot code executed by the processor to authenticate the certificate and to compare ~~validate~~ the regenerated signature digest with the received signature digest.

12. (Original) The apparatus of claim 11, wherein the first and second storage units and the processor are implemented within an integrated circuit.

13. (Original) The apparatus of claim 9 and implemented within a wireless communication device.

14. (Currently Amended) An apparatus having validation of an association of ~~operable to validate~~ software code with [[for]] hardware, comprising:

means for obtaining a certificate from a code image, wherein:

the code image further including software code, a code signature, and a first identifier associated with a release of the software code,

all instances of the software code associated with the software release have the same first identifier such that at least two instances of the software code have the same first identifier,

the code signature is generated, using cryptography and a code private key, based on the first identifier, a second identifier for the hardware, and a message code digest obtained by hashing the software code,

the code signature is used to validate an association of the software code with the hardware,

the certificate includes a code public key corresponding to the code private key, and an authority signature generated over the code public key using cryptography and an authority private key;

means for authenticating the [[a]] certificate~~, sent with a code image including the software, using~~ with an authority ~~first~~ public key securely stored in the hardware~~, wherein the certificate includes a signature and a second public key, and the certificate is included in a code image~~;

means for obtaining the first identifier from the code image;

means for obtaining the second identifier for the hardware, wherein all instances of a particular configuration of the hardware have the same second identifier such that at least two instances of the hardware have the same second identifier;

means for obtaining the software code from the code image and generating an image code digest by hashing the software code from the code image;

generating a regenerated signature digest by hashing the image code digest, the first identifier, and the second identifier; and

means for obtaining the code [[a]] signature[[,]] from the code image and generating a received signature digest by decrypting the code signature from the code image using the code public key~~ certificate, generated for the software, a first identifier for the software, and a second identifier for the hardware, wherein the signature is generated using cryptography and is used to validate an association of the software with the hardware~~; and

means for comparing ~~validating~~ the regenerated signature digest with the received signature digest ~~a second public key from the certificate~~, wherein the association of the software code with the hardware is validated if the regenerated signature digest matches the received signature digest ~~is validated~~.

15-35. (Canceled)

36. (Previously Presented) An apparatus operable to validate software for hardware, comprising:

a storage device configured to store a code image including the software, a code signature, and a certificate;

a secure storage device configured to store a hardware identifier and a certificate authority public key;

a processor configured to access the storage device and operative to:

authenticate the certificate with the certificate authority public key,

obtain a regenerated signature digest based on the software, a first identifier for the software, and the hardware identifier,

decrypt the certificate using the certificate authority public key to recover a code public key,

decrypt the code signature using the code public key to recover a received signature digest, and

compare the regenerated signature digest with the received signature digest to validate the association of the software with the hardware.

37. (Previously Presented) The apparatus of claim 36, wherein the hardware identifier and the certificate authority public key are embedded in the apparatus in a tamper-proof manner.

38. (Currently Amended) The apparatus of claim 1, wherein the authority ~~first~~ public key is embedded in the hardware in a tamper-proof manner.

39. (Currently Amended) The apparatus of claim 9, wherein the authority ~~first~~ public key is embedded in the hardware in a tamper-proof manner.

40. (Currently Amended) The apparatus of claim 14, wherein the authority ~~first~~ public key is embedded in the hardware in a tamper-proof manner.

41. (New) A processor associated product, comprising:

processor-readable medium, comprising:

software code for causing a processor to obtain a certificate from a code image, wherein:

the code image further including software code, a code signature, and a first identifier associated with a release of the software code,

all instances of the software code associated with the software release have the same first identifier such that at least two instances of the software code have the same first identifier,

the code signature is generated, using cryptography and a code private key, based on the first identifier, a second identifier for the hardware, and a message code digest obtained by hashing the software code,

the code signature is used to validate an association of the software code with the hardware,

the certificate includes a code public key corresponding to the code private key, and an authority signature generated over the code public key using cryptography and an authority private key;

software code for causing a processor to authenticate the certificate with an authority public key securely stored in the hardware;

software code for causing a processor to obtain the first identifier from the code image;

software code for causing a processor to obtain the second identifier for the hardware, wherein all instances of a particular configuration of the hardware have the

same second identifier such that at least two instances of the hardware have the same second identifier;

software code for causing a processor to obtain the software code from the code image and generate an image code digest by hashing the software code from the code image;

software code for causing a processor to generate a regenerated signature digest by hashing the image code digest, the first identifier, and the second identifier; and

software code for causing a processor to obtain the code signature from the code image and generate a received signature digest by decrypting the code signature from the code image using the code public key; and

software code for causing a processor to compare the regenerated signature digest with the received signature digest, wherein the association of the software code with the hardware is validated if the regenerated signature digest matches the received signature digest.

42. (New) The processor associated product of claim 41, wherein the authority public key is embedded in the hardware in a tamper-proof manner.